PAT-NO: JP02002101091A

DOCUMENT-IDENTIFIER: **JP 2002101091 A**

TITLE: USER AUTHENTICATION METHOD AND USER AUTHENTICATION PROGRAM

PUBN-DATE: April 5, 2002

INVENTOR-INFORMATION:

NAME	COUNTRY
TAHIRA, YOSHITOMO	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
HITACHI INFORMATION SYSTEMS LTD	N/A

APPL-NO: JP2000288596

APPL-DATE: September 22, 2000

INT-CL (IPC): H04L009/32, G06F015/00 , H04Q007/34

ABSTRACT:

PROBLEM TO BE SOLVED: To realize user authentication the security of which is high, and to save charge for the communication fee of a portable telephone for receiving an on-line information service, and to use the portable telephone for other purposes, even while receiving the on-line information service.

SOLUTION: The present **position** information of a user from a base station 109, which presents the service of the present **position** information of a portable telephone 107, is compared with the **position** information of a client machine 102 which requests the on-line information service, and when they agree, it is determined that the user is definitely the individual himself, so that user **authentication** can be carried out by a server 105. There are two cases, in which the client machine itself is provided with a **GPS** 103 in one case, and the set place information of the client machine 102 is registered in the server in the other case, so that the positional information of the client machine can be acquired.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－101091
（P2002－101091A）
(43)公開日　平成14年４月５日(2002.4.5)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　9/32		Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０８５
Ｇ０６Ｆ　15/00	３３０	Ｈ０４Ｌ　9/00	６７３Ａ	５Ｊ１０４
Ｈ０４Ｑ　7/34			６７３Ｂ	５Ｋ０６７
			６７５Ｄ	
		Ｈ０４Ｑ　7/04	Ｃ	

審査請求　有　請求項の数４　ＯＬ　（全７頁）

(21)出願番号　特願2000－288596(P2000－288596)

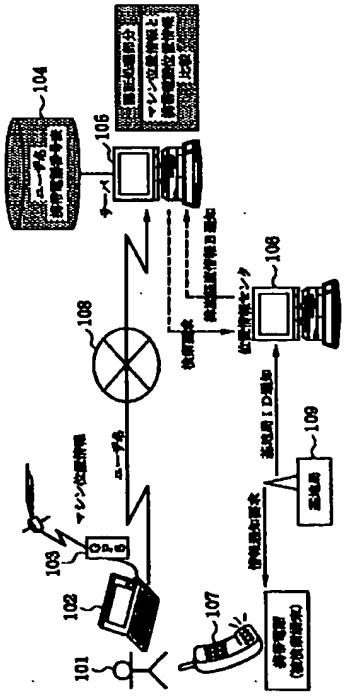
(22)出願日　平成12年９月22日(2000.9.22)

(71)出願人　000152985
株式会社日立情報システムズ
東京都渋谷区道玄坂１丁目16番５号
(72)発明者　田平　良知
東京都渋谷区道玄坂一丁目16番５号　株式会社日立情報システムズ内
(74)代理人　100077274
弁理士　磯村　雅俊　（外１名）

Ｆターム(参考)　5B085 AA08 AE00 AE02
5J104 AA07 KA01 KA20 MA01 NA01 PA10
5K067 AA32 BB04 DD17 DD20 EE04 EE10 HH22

(54)【発明の名称】　ユーザ認証方法およびユーザ認証プログラム

(57)【要約】
【課題】セキュリティの高いユーザ認証を得ることができ、オンライン情報サービスを受けるために携帯電話の通信料の負担がなく、オンライン情報サービスを受けている間も携帯電話をそれ以外に利用できるようにする。
【解決手段】携帯電話１０７の現在位置情報をサービスする基地局１０９からのユーザの現在位置情報と、オンライン情報サービスの要求を行うクライアントマシン１０２の位置情報との比較により、一致すれば確かに本人であると判別してサーバ１０５がユーザ認証を行う。クライアントマシンの位置情報の取得には、クライアントマシン自身にＧＰＳ１０３を備える場合と、サーバに予めクライアントマシン１０２の設置場所情報を登録しておく場合とがある。



1

【特許請求の範囲】

【請求項1】　ユーザＩＤに対応して該ユーザの携帯型電話の番号を格納した情報をサーバコンピュータに有し、

前記サーバコンピュータは、ネットワークを介して接続されたクライアントコンピュータから入力されたユーザＩＤおよび該クライアントコンピュータの位置情報とを受取り、

前記ユーザＩＤに基づいて前記情報を参照し、対応する携帯型電話の番号を検索し、

検索された携帯型電話の番号に基づいて、該携帯型電話の現在位置情報を取得し、

取得した携帯型電話の位置情報と前記クライアントコンピュータから受取った位置情報とを比較して、比較の結果が一致することによりユーザ認証をすることを特徴とするユーザ認証方法。

【請求項2】　ユーザＩＤに対応して該ユーザの携帯型電話の番号を格納した第１の情報と、クライアントコンピュータに対応して該クライアントコンピュータの位置情報を格納した第２の情報とをサーバコンピュータに有し、

前記サーバコンピュータは、ネットワークを介して接続されたクライアントコンピュータから入力されたクライアントコンピュータＩＤおよびユーザＩＤを受取り、

受取ったユーザＩＤに基づいて前記第１の情報を参照し、対応する携帯型電話の番号を検索し、

受取ったクライアントコンピュータＩＤに基づいて前記第２の情報を参照し、対応する位置情報を検索し、

一方、前記検索された携帯型電話の番号に基づいて、該携帯型電話の現在位置情報を取得し、

取得した携帯型電話の位置情報と前記第２の情報を検索して求めた位置情報とを比較して、比較の結果が一致することによりユーザ認証をすることを特徴とするユーザ認証方法。

【請求項3】　クライアントコンピュータとネットワークを介して接続されたサーバコンピュータ内で動作するユーザ認証プログラムであって、

前記クライアントコンピュータから入力されたユーザＩＤと前記クライアントコンピュータから送信された該クライアントコンピュータの位置情報とを受取る処理と、

受取ったユーザＩＤに基づいて、ユーザＩＤに対応して該ユーザの携帯型電話の番号を格納した情報を参照し、対応する携帯型電話の番号を検索する処理と、

検索された携帯型電話の番号に基づいて該携帯型電話の現在位置情報を取得する処理と、

取得した携帯型電話の位置情報と前記クライアントコンピュータから受取った位置情報とを比較する処理とを有することを特徴とするユーザ認証プログラム。

【請求項4】　クライアントコンピュータとネットワークを介して接続されたサーバコンピュータ内で動作するユーザ認証プログラムであって、

2

前記クライアントコンピュータから入力されたクライアントコンピュータＩＤおよびユーザＩＤを受取る処理と、

受取ったユーザＩＤに基づいて、ユーザＩＤに対応して該ユーザの携帯型電話の番号を格納した第１の情報を参照し、対応する携帯型電話の番号を検索する処理と、

受取ったクライアントコンピュータＩＤに基づいて、前記クライアントコンピュータに対応して該クライアントコンピュータの位置情報を格納した第２の情報を参照し、対応する位置情報を検索する処理と、

検索された携帯型電話の番号に基づいて該携帯型電話の現在位置情報を取得する処理と、

取得した携帯型電話の位置情報と前記第２の情報を検索して求めた位置情報とを比較する処理とを有することを特徴とするユーザ認証プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ユーザ認証方法およびそのプログラムに係り、特に携帯型電話および現在位置情報を用いてユーザを認証する方法およびユーザ認証プログラムに関する。

【０００２】

【従来の技術】従来、クライアント／サーバ型のシステムを使ったオンライン情報サービスが広く普及している。このようなオンライン情報サービスは、予め登録されているユーザに対してのみサービスの利用を許可する場合が多い。サービスを利用しようとするユーザは、ユーザ名およびパスワードをクライアントコンピュータから入力し、この情報に基づいてサーバコンピュータがユーザを認証してはじめてサービスの利用が許可されるのが一般的である。従来より認証の方法に関する技術は種々あるが、その中の一つに、最近、普及が目覚しい携帯電話を利用したユーザ認証技術がある。これについては例えば、特開２０００-７８２８０号公報に書かれたものが知られている。これは、情報提供サービスを行う情報センタ等にアクセスしてくる端末装置の認証に関する技術であり、まず端末装置はユーザIDと共に携帯電話機の電話番号を情報センタに送る。情報センタの認証装置は認証用メモリに記憶されている電話番号によりユーザ認証を行い、OKならば情報提供サービスを行うものである。ここで情報提供サービスとして、例えばオンライン情報サービスなどがユーザから要望されている。

【０００３】一方、認証技術が用いられるオンライン情報サービスの一例として、現金自動取引装置のキャッシュカードによる取引サービスがある。ユーザは、取引に際して現金自動取引装置にキャッシュカードを挿入し、暗証番号を入力する。入力された暗証番号に基づいて認証が実施され、OKならばその後の処理が実施される。しかし、このような認証処理では、偽のカード所有者が何

らかの方法で暗証番号を知ることにより、取引サービスが許可されてしまう。本人が紛失、盗難に気付いていない状況にあっても、カードが使用される時点で、その不正使用の有無をチェックし、或いはその使用を否とするようなカードシステムについて、例えば特開平11－96323号公報に書かれた技術が知られている。これは、カードのデータ記憶部に、顔写真画像データ，本人指定電話番号，カード管理センタ電話番号を記憶しておき、カード利用端末にカードの使用時にデータ記憶部から読み取った本人指定電話番号に自動ダイヤルして、カード使用中を知らせるメッセージを発信するメッセージ送受信部を設けてチエックするものである。他方、携帯電話を利用したサービスとして、携帯電話が通話中でなくても常に近辺の基地局と交信できることを利用して、携帯電話の現在位置情報を取得するサービスが提供されており、これに関しては例えば特開平11－331922号公報に記載された技術が知られている。このサービスでは、基地局から呼び出すことにより徘徊老人の現在位置を知ることができる。

【0004】

【発明が解決しようとする課題】しかしながら、前述の従来技術においては、下記のような問題点がある。すなわち、上記特開2000-78280号公報記載の技術では、オンライン情報サービスを予め登録された電話番号のみに制限する技術であるため、悪意を持つ者が、サービスを利用できるユーザ（つまり、予め登録を受けた電話番号を持つユーザ）の携帯電話を盗んでこれを利用すればサービスを利用できてしまうという問題がある。また、上記従来技術によれば、携帯電話を介してオンライン情報サービスを受ける為には、携帯電話の電話料金が必要であった。特に、LAN環境に接続されて電話回線を通常利用しなくてもオンライン情報サービスを享受できる環境においても、携帯電話の電話料金が必要になることは、ユーザに大きな負担であった。一方、特開平11－96323号公報に書かれた技術によれば、カードを使用する度に登録された電話番号、例えば携帯電話の番号に電話がかかるため、真の利用者はこれに対して何がしかの応答を返さなければならず、極めて煩わしいという問題がある。

【0005】そこで、本発明の目的は、これら従来の課題を解決し、セキュリティの高いユーザ認証を得ることができ、かつ利用者が煩わしい思いをせず、またオンライン情報サービスを受けるために携帯電話の通信料の負担がなく、しかもオンライン情報サービスを受けている間も携帯電話をそれ以外に利用することが可能なユーザ認証方法およびユーザ認証プログラムを提供することにある。

【0006】

【課題を解決するための手段】上記目的を達成するため、本発明のユーザ認証方法では、携帯電話の現在位置情報を取得するサービスを利用して取得したオンライン情報サービスを要求したユーザの現在位置情報と、オンライン情報サービスの要求を行う（クライアント）マシンの位置情報との比較により、一致すれば確かに本人であると判別してユーザ認証を行うものである。クライアントマシンの位置情報の取得には、第1の実施例として、クライアントマシン自身にGPS（Global Positioning System）情報を取得する機能を備えている場合には、上記GPS情報を利用する方法を用い、そうでない場合を第2の実施例として、サーバに予めクライアントマシンの設置場所情報を登録しておく方法を用いる。また、上記と同じ動作を行うプログラムをコンピュータにインストールすることにより、本発明を容易に実現する。これにより、操作者はオンライン情報サービスを受けるために、携帯電話の通信料の負担がなく、かつ煩わしい操作もなく、またオンライン情報サービスを受けている間でも、携帯電話をオンライン情報サービス以外に利用することができるという効果がある。

【0007】

【発明の実施の形態】以下、本発明の実施例を、図面により詳細に説明する。

（第1の実施例）図1は、本発明の第1の実施例を示すユーザ認証システムの構成図である。第1の実施例は、クライアントマシン102自身にGPS（Global Positioning System）103の情報を取得する機能を備えている場合である。操作者101は、GPS103を接続したクライアントマシン102と、別個に携帯電話機107を備えているものとする。クライアントマシン102の操作者101がネットワーク108を介してサーバ105にオンラインサービスを要求する際には、操作者101がGPS103を用いてクライアントマシン102の現在位置情報を取得し、取得した現在位置情報をユーザ名とともにサーバ105に送信する。サーバ105には、ユーザ名と携帯電話番号を対にして登録したテーブル（ユーザ名携帯電話番号表）104が備えられている。

【0008】サーバ105では、送信されてきたユーザ名に対応する登録済の携帯電話の電話番号をユーザ名携帯電話番号表104から取得する。次に、位置情報センタ106に対して、前記取得した携帯電話の現在位置情報の取得を要求（検索要求）する。位置情報センタ106は、該携帯電話107と交信を行っている基地局109から携帯電話107の所在地を取得し、サーバ105に返却する。このために、位置情報センタ106は、先ず携帯電話107と交信を行っている基地局109から基地局IDの通知を受け、基地局109は被検索端末である携帯電話107に対して情報通知要求を送信して現在位置の情報を取得した後、位置情報センタ106に送信する。位置情報センタ106は、受信した携帯電話107の現在位置情報（経度緯度情報）をサーバ105に

返送する。サーバ１０５では、クライアントマシン１０２から送られてきたマシンの現在位置情報を位置情報センタ１０６から送られてきた携帯電話の所在地とを比較して、ユーザ名携帯電話番号表１０４に登録された電話番号の携帯電話を持っている人がオンラインサービスを要求したか否かを判断する。一致すれば、同一人が要求したと判別し、ユーザ認証を行う。

【０００９】（第２の実施例）図２は、本発明の第２の実施例を示すユーザ認証システムの構成図である。図１の第１の実施例との違いは、図１では、ＧＰＳ１０３を用いてクライアントマシン自身でクライアントマシン１０２の現在位置情報を取得しているのに対して、図２の第２の実施例では、サーバ１０５のマシン名位置情報対応表２０１にクライアントマシンの設置場所を登録するか、あるいは別にマシン名位置情報対応表２０１を用意しておき、クライアントマシン１０２からは、マシン位置情報の代りにユーザ名とマシン名をサーバ１０５に送信するようにしたものである。クライアントマシン１０２の操作者１０１がネットワーク１０８を介してサーバ１０５にオンラインサービスを要求する際には、操作者１０１はユーザ名とともにマシン名をサーバ１０５に送信する。サーバ１０５には、ユーザ名と携帯電話番号を対にして登録したテーブル（ユーザ名携帯電話番号表）１０４の他に、マシン名とそのクライアントマシンの位置情報を対にして登録したマシン名位置情報対応表２０１が備えられている。サーバ１０５では、送信されてきたユーザ名に対応する登録済の携帯電話の電話番号をユーザ名携帯電話番号表１０４から取得する。次に、位置情報センタ１０６に対して、前記取得した携帯電話の現在位置情報の取得を要求（検索要求）する。

【００１０】位置情報センタ１０６は、該携帯電話１０７と交信を行っている基地局１０９から携帯電話１０７の所在地を取得し、サーバ１０５に返却する。このために、位置情報センタ１０６は、先ず携帯電話１０７と交信を行っている基地局１０９から基地局ＩＤの通知を受け、基地局１０９は被検索端末である携帯電話１０７に対して情報通知要求を送信して現在位置の情報を取得した後、位置情報センタ１０６に送信する。位置情報センタ１０６は、受信した携帯電話１０７の現在位置情報（経度緯度情報）をサーバ１０５に返送する。サーバ１０５は、クライアントマシン１０２から送られてきたマシン名を基にマシン名位置情報対応表２０１から現在位置情報を取り出し、その現在位置情報と位置情報センタ１０６から送られてきた携帯電話の所在地とを比較して、ユーザ名携帯電話番号表１０４に登録された電話番号の携帯電話を持っている人がオンラインサービスを要求したか否かを判断する。一致すれば、同一人が要求したと判別し、ユーザ認証を行う。

【００１１】図３は、図１および図２における認証処理部分の動作フローチャートである。認証処理は、サーバ１０５にある認証プログラムが動作することにより行われる。まず、マシン名を受信したか否かを判断し（ステップ３０１）、マシン名を受信した場合には、マシン名位置情報対応表２０１から予め登録されているマシン名に対応するマシンの位置情報を取得する（ステップ３０２）。一方、マシン名を受信しない場合には、第１の実施例のようにユーザから現在位置情報が送られてくるので、それを受信する。次に、ユーザ名携帯電話番号表１０４をユーザ名で検索して、対応するユーザが所持しているであろう携帯電話の電話番号を取得する（ステップ３０３）。次に、位置情報センタからステップ３０３で取得した携帯電話の現在位置を取得する（ステップ３０４）。次に、クライアントマシンから送られてきたクライアントマシンの位置情報、またはステップ３０２で取得したマシン位置情報と、ステップ３０４で取得した携帯電話の位置情報とを比較して（ステップ３０５）、一致した場合には正規のユーザからの要求と判断し（ステップ３０６）、一致しない場合には、正規のユーザからの要求でないと判断する（ステップ３０７）。

【００１２】以上示したように、本発明によれば、携帯電話を通してオンラインサービスを行うものではないので、オンラインサービス中の通信料が付加されることはない。また、携帯電話の電源が入っているときのみアクセス可能とするように、制限を加えることもできる。また、携帯電話の位置以外からアクセス要求があった場合、サーバから携帯電話へ不正使用の可能性が有る旨のメールの送信を行うこともできる。これらの機能を追加することにより、不正な者からの悪用を防止することができる。さらに、従来からのユーザ名、パスワードといったユーザ認証方法と組み合わせて使用することもできる。

【００１３】（第３の実施例）図４は、本発明の第３の実施例を示すユーザ認証システムの構成図であって、クレジットカードの認証に適用した例を示す。図４においては、クレジットカードの認証を携帯電話の現在位置情報の一致（ここでは、交信する基地局ＩＤの一致）により行う方法である。サーバ４０５側には、予め各店舗におかれた各端末４０２のマシン名とこの端末の設置場所に対応する携帯電話の基地局（基地局ＩＤ）とを対応付けて格納したテーブル４１０と、クレジットカード申し込み時にユーザの携帯電話番号とユーザＩＤとを対応付けたテーブル４０４とが設置されている。利用者がクレジットカードを使って買い物をすると、店舗に置かれた端末４０２から本人認証を行うための情報として、マシン名とユーザＩＤ、またはマシン名とクレジットカード番号（カードＩＤ）がサーバコンピュータ４０５へ送信される。サーバコンピュータ４０５では、受取った情報に基づいて、テーブル４０４からユーザの携帯電話番号を検索する。検索された電話番号の携帯電話と交信している基地局を位置情報センタ４０６へ問い合わせる（検

索要求）。位置情報センタ４０６は、該携帯電話４０７と交信を行っている基地局４０９の基地局ＩＤを取得し、これをサーバ４０５に返却する。サーバ４０５は、店舗のクライアントマシン４０２から送られてきたマシン名を基にテーブル４１０から基地局ＩＤを取り出し、その基地局ＩＤと位置情報センタ１０６から送られてきた基地局ＩＤとを比較して、一致か不一致かによりテーブル４０４に登録された電話番号の携帯電話を持っている人がマシン名の設置した店舗で使用されたクレジットカードであるか否かを判断する。一致すれば、同一人のクレジットカードであると判別し、カード認証を行う。

【００１４】第１～第３の実施例で説明した位置情報センタ１０６、４０６は別マシンであるが、同一のコンピュータで実施することも勿論可能である。また、第３の実施例では、位置情報として、基地局ＩＤの比較により判断しているが、地図上の座標を用いて現在位置情報どうしを比較して判定することにより、さらに正確に判断することもできる。

【００１５】

【発明の効果】以上説明したように、本発明によれば、セキュリティの高い認証を簡単な操作で受けることができ、オンラインサービスのためのユーザ認証を受けたり、クレジットカードの認証を受けるために、携帯電話の通信料の負担がなく、また、オンラインサービスやクレジットカードの認証を受けている間も携帯電話をオンラインサービス以外に利用することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施例を示すユーザ認証システムの構成図である。

【図２】本発明の第２の実施例を示すユーザ認証システムの構成図である。

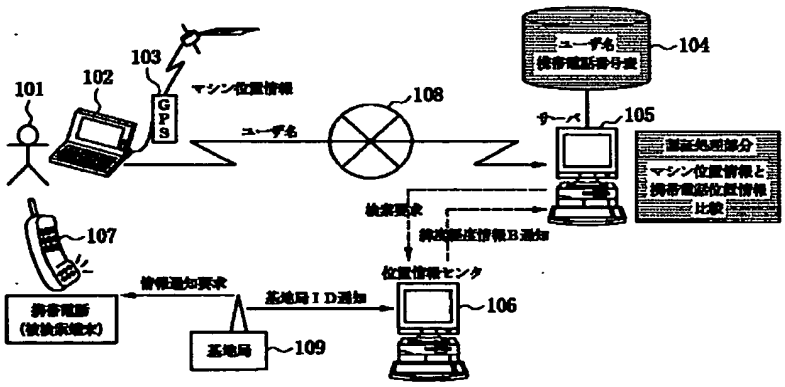
【図３】図１および図２における認証処理部分の動作フローチャートである。

【図４】本発明の第３の実施例を示すもので、図２のサービスをクレジットカード認証に適用した例を示す図である。

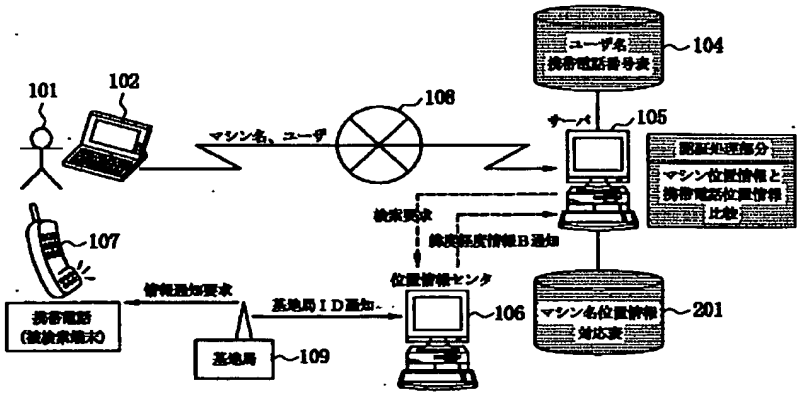
【符号の説明】

１０１，４０１…ユーザ、１０２，４０２…クライアントマシン、１０３…ＧＰＳ、１０４…ユーザ名携帯電話番号表、１０５，４０５…サーバ、１０６，４０６…位置情報センタ、１０７，４０７…携帯電話、１０８，４０８…ネットワーク、１０９，４０９…基地局、２０１…マシン名位置情報対応表、４０４…ユーザＩＤ、カードＩＤ、携帯電話番号登録テーブル、４１０…マシン名、基地局ＩＤ登録テーブル。

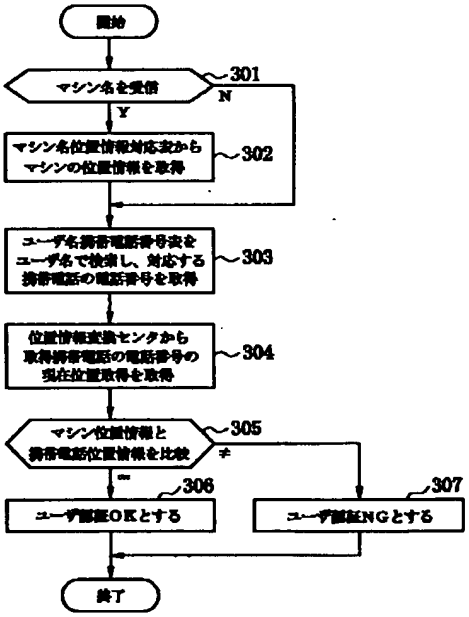
【図１】



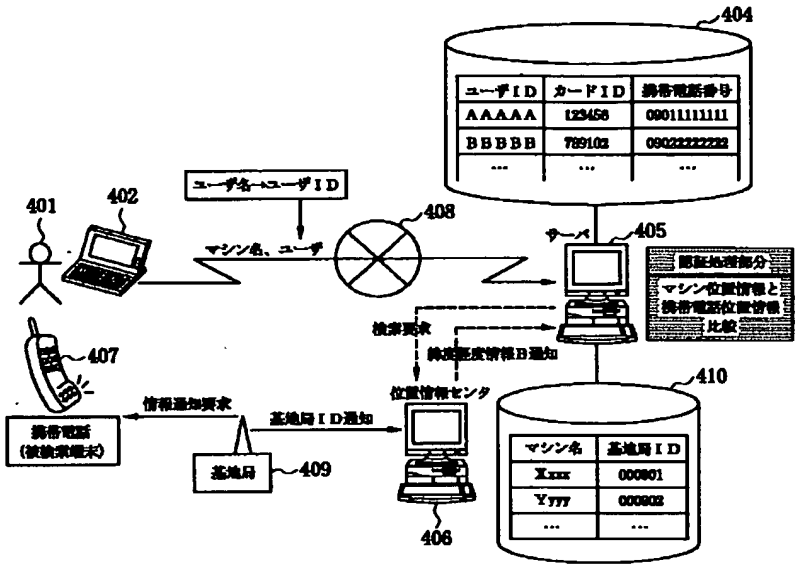
【図2】


101
102
マシン名、ユーザ
108
ユーザ名
携帯電話番号表
104
サーバ
105
認証処理部分
マシン位置情報と
携帯電話位置情報
比較
検索要求
検索結果情報B通知
107
情報通知要求
位置情報センタ
基地局ID通知
106
マシン名位置情報
対応表
201
携帯電話
(被検索端末)
基地局
109

【図3】


開始
マシン名を受信
301
N
Y
マシン名位置情報対応表から
マシンの位置情報を取得
302
ユーザ名携帯電話番号表を
ユーザ名で検索し、対応する
携帯電話の電話番号を取得
303
位置情報変換センタから
取得携帯電話の電話番号の
現在位置取得を取得
304
マシン位置情報と
携帯電話位置情報を比較
305
=
≠
ユーザ認証OKとする
306
ユーザ認証NGとする
307
終了

【図4】


404
ユーザID
カードID
携帯電話番号
AAAAA
123456
09011111111
BBBBB
789102
09022222222
401
402
ユーザ名→ユーザID
マシン名、ユーザ
408
サーバ
405
認証処理部分
マシン位置情報と
携帯電話位置情報
比較
検索要求
検索要求情報B通知
407
位置情報センタ
410
情報通知要求
基地局ID通知
携帯電話
(被検索端末)
基地局
409
マシン名
基地局ID
Xxxx
000001
Yyyy
000002
406